4910-15-U

DEPARTMENT OF HOMELAND SECURITY

COAST GUARD

33 CFR Part 106

[USCG-2003-14759]

RIN 1625-AA68

Outer Continental Shelf Facility Security

AGENCY: Coast Guard, DHS.

ACTION: Temporary interim rule with request for comments and notice of meeting.

SUMMARY: This interim rule provides security measures for mobile offshore drilling units (MODUs) not subject to the International Convention for the Safety of Life at Sea, 1974, (SOLAS) and certain fixed and floating facilities on the Outer Continental Shelf (OCS) other than deepwater ports. For the purpose of this part, non-SOLAS MODUs and certain fixed and floating facilities on the OCS are collectively referred to as OCS facilities. This rule requires the owners or operators of OCS facilities to designate security officers, develop security plans based on security assessments, implement security measures specific to the OCS facility's operation and comply with Maritime Security Levels. This interim rule is one of six

interim rules in today's Federal Register that comprise a new subchapter on the requirements for maritime security mandated by the Maritime Transportation Security Act of 2002. These six interim rules implement national maritime security initiatives concerning General Provisions, Area Maritime Security (ports), Vessels, Facilities, OCS Facilities, and the Automatic Identification System. Where appropriate, they align these domestic maritime security requirements with those of the International Ship and Port Facility Security (ISPS) Code and recent amendments to SOLAS. This interim rule will benefit persons and property by requiring security plans and procedures to prevent, deter, detect, and respond to incidents that threaten the security of OCS facilities. To best understand these rules, first read the one titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792).

DATES:

Effective date. This interim rule is effective from [Insert date of publication in the FEDERAL REGISTER.] until November 25, 2003.

Comments. Comments and related material must reach the Docket Management Facility on or before [Insert date 30 days after date of publication in the FEDERAL REGISTER.]. Comments on collection of information sent to the Office of

Management and Budget (OMB) must reach OMB on or before [Insert date 30 days after date of publication in the FEDERAL REGISTER.].

Meeting. A public meeting will be held on July 23, 2003, from 9 a.m. to 5 p.m., in Washington, DC.

ADDRESSES:

Comments. To make sure that your comments and related material are not entered more than once in the docket, please submit them by only one of the following means:

(1) Electronically to the Docket Management System website at http://dms.dot.gov;

(2) By mail to the Docket Management Facility (USCG-2003-14759), U.S. Department of Transportation, room PL-401, 400 Seventh Street SW., Washington, DC 20590-0001;

(3) By fax to the Docket Management Facility at 202-493-2251; or

(4) By delivery to room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

You must also mail comments on collection of information to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street

NW., Washington, DC 20503, ATTN: Desk Officer, U.S. Coast Guard.

Meeting. A public meeting will be held on July 23, 2003, in Washington, DC, at the Grand Hyatt Washington, DC, 1000 H Street, NW., Washington, DC 20001.

Availability. Electronic forms of all comments received into any of our dockets can be searched by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor unit, etc.) and is open to the public without restriction. You may also review the Department of Transportation's complete Privacy Act Statement published in the Federal Register on April 11, 2000(65 FR 19477-78), or you may visit http://dms.dot.gov/.

FOR FURTHER INFORMATION CONTACT: If you have questions on this rule, call Lieutenant Greg Versaw by telephone 202-267-1103, toll-free telephone 1-800-842-8740 ext. 7-1103, or electronic mail msregs@comdt.uscg.mil. If you have questions on viewing or submitting material to the docket, call Ms. Dorothy Beard, Chief, Dockets, Department of Transportation, telephone 202-366-5149.

SUPPLEMENTARY INFORMATION:

Due to the short timeframe given to implement these National Maritime Transportation Security initiatives, as

directed by the Maritime Transportation Security Act (MTSA) of 2002 (MTSA, Public Law 107-295, 116 STAT. 2064), and to ensure all comments are in the public venue for these important rulemakings, we are not accepting comments containing protected information for these interim rules. We request you submit comments, as explained in the Request for Comments section below, and discuss your concerns or support in a manner that is not security sensitive. We also request that you not submit proprietary information as part of your comment.

The Docket Management Facility maintains the public docket for this rulemaking. Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, will be available for inspection or copying at room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at http://dms.dot.gov.

Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related material. Your comments will be considered for the final rule we plan to issue before November 25, 2003, to replace this interim rule. If

you choose to comment on this rule, please include your name and address, identify the specific docket number for this interim rule (USCG-2003-14759), indicate the specific heading of this document to which each comment applies, and give the reason for each comment. You may submit your comments and material by mail, hand delivery, fax, or electronic means to the Docket Management Facility at the address under ADDRESSES. Please submit your comments and material by only one means. If you submit them by mail or hand delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period. We may change this interim rule in view of them.

Public Meeting

We will hold a public meeting on July 23, 2003, in Washington, DC, at the Grand Hyatt Hotel, at the address listed under ADDRESSES. The meeting will be from 9 a.m. to 5 p.m. to discuss all of the maritime security interim rules, and the Automatic Identification System (AIS) interim rule found in today's Federal Register. In addition, you may submit a request for other public

meetings to the Docket Management Facility at the address under ADDRESSES explaining why another one would be beneficial. If we determine that other meetings would aid this rulemaking, we will hold them at a time and place announced by a later notice in the Federal Register.

Regulatory Information

We did not publish a notice of proposed rulemaking (NPRM) for this rulemaking and are making this interim rule effective upon publication. Section 102(d)(1) of the MTSA requires the publication of an interim rule as soon as practicable without regard to the provisions of chapter 5 of title 5, U.S. Code (Administrative Procedure Act). The Coast Guard finds that harmonization of U.S. regulations with maritime security measures adopted by the International Maritime Organization (IMO) in December 2002, and the need to institute measures for the protection of U.S. maritime security as soon as practicable, furnish good cause for this interim rule to take effect immediately under both the Administrative Procedure Act and section 808 of the Congressional Review Act.

Background and Purpose

A summary of the Coast Guard's regulatory initiatives for maritime security can be found under the Background and Purpose section in the preamble to the interim rule titled

"Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

Discussion of Comments Addressing OCS Facility Issues in the Notice of Meeting

For a discussion of comments on OCS facilities at the public meetings and in the docket, see the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

Discussion of Interim Rule

This interim rule regulates the owners and operators of OCS facilities to provide security to these OCS facilities and to other vessels with which an OCS facility interfaces. The interim rule adds new 33 CFR part 106, OCS Facility Security, as part of 33 CFR, Chapter I, subchapter H, Maritime Security. A general description of the process used in developing subchapter H and its component parts appears in the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792).

This interim rule applies to Certificated Mobile Offshore Drilling Units (MODUs) that are not subject to International Convention for Safety of Life at Sea, 1974, (SOLAS) and fixed or floating platforms operating on the

Outer Continental Shelf that host more than 150 persons for 12 hours or more during each 24-hour period continuously for 30 days or more, or produce more than 100,000 barrels of oil per day, and/or produce more than 200 million cubic feet of natural gas per day. OCS facilities that do not meet these characteristics may still be required to conduct a Facility Security Assessment, develop a Facility Security Plan, and implement certain security measures if the cognizant Coast Guard District Commander makes that determination. That determination is made on a case-by-case basis, based upon unique local conditions, specific intelligence information, or other identifiable and articulable risk factors that confirm such actions are necessary and appropriate to ensure an adequate level of security. This requirement would be issued in a Maritime Security Directive. This interim rule does not apply to deepwater ports.

The MTSA and the International Ship and Port Facility Security (ISPS) Code use different terms to define similar, if not identical, persons or things. These differing terms sometimes match up with the terms used in subchapter H, but sometimes they do not. For a table of the terms used in subchapter H and their related terms in the MTSA and the ISPS Code, see the Discussion of Interim Rule section in

the preamble for the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), published elsewhere in today's Federal Register.

The purpose of this rulemaking is to require certain OCS facilities to perform security assessments, develop security plans, and implement security measures and procedures to reduce the risk of and to mitigate the results of an act that threatens the security of the OCS facility, the crew, or the public. This rulemaking combines international requirements and existing domestic policy, and is published as a part of a new subchapter on maritime security. The MTSA mandates that OCS facilities conduct security assessments and develop security plans, submit these plans within 6 months of publication of this interim rule. It also mandates that each OCS facility shall be in compliance with its approved security plans within 12 months of the publication of this interim rule.

Part 106 consists of four subparts: subpart A (General), subpart B (Security Requirements), subpart C (OCS Facility Security Assessment), and subpart D (OCS Facility Security Plan). The requirements discussed in part 106 are consistent with similar requirements in parts 104 and 105 of this subchapter. These interim rules include requirements discussed below.

Waivers.

The waiver section of this interim rule establishes procedures for OCS facility owners or operators who wish to be relieved of complying with specific requirements of the interim rule on the grounds that those requirements are unreasonable or unnecessary.

Equivalents.

The equivalents section of this interim rule establishes procedures for requesting an equivalency to the requirements of this interim rule. Equivalencies are intended to allow an OCS facility owner or operator to provide an alternative provision or arrangement that provides the same level of security as a specific requirement contained within this part.

Alternatives.

The alternatives section of this interim rule allows OCS facility owners or operators to implement an Alternative Security Program that has been reviewed and accepted by the Commandant (G-MP) to meet the requirements of this part. An Alternative Security Program must be comprehensive and must be demonstrated to meet the intent of each section of this part. Owners or operators are required to implement an Alternative Security Program in its entirety to be deemed in compliance with this part.

Appeals.

The appeals section of this interim rule establishes the procedures for OCS facility owners or operators who are aggrieved by, and wish to contest, a Coast Guard decision regarding a matter covered by this interim rule.

Owner or Operator Responsibilities.

The owner or operator of a facility is generally responsible for all requirements imposed by this part. The owner or operator must:

- Ensure the performance of all OCS facility security duties;
- Define the security organizational structure for each OCS facility and provide each person exercising security duties or responsibilities within that structure with the support needed to fulfill those obligations;
- Designate, by name or title, a Company Security Officer and a Facility Security Officer for each OCS facility;
- Ensure that a Facility Security Assessment is conducted;
- Ensure the development and submission for approval of a Facility Security Plan.

- Ensure that the OCS facility operates in compliance with the approved Facility Security Plan;
- Ensure that adequate coordination of security issues takes place between the OCS facility and vessels, including the execution of a Declaration of Security;
- Ensure that security communication is readily available;
- Ensure coordination with and implementation of changes in MARSEC Level; and
- Ensure all breaches of security and security incidents are reported.

Company Security Officer (CS0).

This interim rule requires that each OCS facility owner or operator appoint a Company Security Officer, designated in writing, for each OCS facility. The Company Security Officer may be a full-time or collateral position. A Company Security Officer may perform other duties within the owner or operator's organization provided he or she is able to perform the duties and responsibilities required of the Company Security Officer.

The Company Security Officer must have a general knowledge in matters of a range of issues, such as company security administration and organization, relevant laws and

regulations, current security threats and patterns, risk assessment methodology, and conducting audits, inspections, and control procedures. The Company Security Officer may delegate his or her duties, but remains responsible for the performance of those duties. The duties of the Company Security Officer include:

- Ensuring that a Facility Security Assessment is carried out;
- Ensuring that a Facility Security Plan is developed, approved, maintained, and implemented;
- Ensuring that the Facility Security Plan is modified when necessary;
- Ensuring that OCS facility security activities are audited and reviewed;
- Ensuring the timely correction of problems identified by audits, reviews, or inspections;
- Ensuring adequate security training; and
- Ensuring communication and cooperation between the OCS facility and vessels.

Facility Security Officer (FSO).

This interim rule requires that the owner or operator of OCS facilities appoint, and designate in writing, a Facility Security Officer. The Facility Security Officer

may be a full-time or collateral position. The Facility Security Officer must have a general knowledge in a range of issues such as security administration and organization, relevant laws and regulations, current security threats and patterns, risk assessment methodology, and conducting audits, inspections, and control procedures. The most important duties a Facility Security Officer must perform include implementing a Facility Security Plan, ensuring that adequate training is provided to OCS facility personnel; ensuring that the OCS facility operates in accordance with the plan and in continuous compliance with part 106; and periodically auditing and updating the Facility Security Assessment and Facility Security Plan. The Facility Security Officer may assign security duties to other OCS facility personnel; however, the Facility Security Officer remains responsible for these duties.

Training.

Required training for OCS facility personnel must be specified in the Facility Security Plan. The Coast Guard will not require specific security training courses for the Facility Security Officer and OCS facility personnel. While formal training may be appropriate, we are not mandating specifics. OCS facility owners or operators must certify that security personnel are, in fact, properly

trained to perform their duties. The types of training required must also be consistent with the training requirements described in this part. The Facility Security Officer is also required to ensure that OCS facility security persons possess necessary training to maintain the overall security of the OCS facility.

Drill and Exercise Requirements.

Exercises are required to ensure the adequacy of the Facility Security Plan and are required to be conducted at least once each calendar year, with no more than 18 months between exercises. Drills, which are smaller in scope than exercises, must be conducted at least every three months. Exercises may be OCS facility specific, or as part of a cooperative exercise program. Exercises for security may be combined with other required exercises, as appropriate.

Security Systems and Equipment Maintenance.

Procedures and/or policies must be developed and implemented to ensure security systems and equipment are tested and operated in accordance with the instructions of the manufacturer and ready for use.

Security Measures.

Security measures for specific activities must be scalable in order to provide increasing levels of security at increasing MARSEC levels. An effective security program

relies on detailed procedures that clearly indicate the preparation and prevention activities that will occur at each threat level and the organizations, or personnel, who are responsible for carrying out those activities. Security Measures must be developed for the following activities:

- Security measures for access control;
- Security measures for restricted areas;
- Security measures for delivery of stores and industrial supplies; and
- Security measures for monitoring.

Declaration of Security (DoS).

This interim rule requires the execution of a Declaration of Security under certain security conditions. A Declaration of Security provides a means for ensuring that critical security concerns are properly addressed prior to a vessel-to-facility interface. Security must be properly addressed by delineating responsibilities for security arrangements and procedures between a vessel and the OCS facility. This obligation is similar to the existing U.S. practice for vessel-to-facility oil transfer procedures.

Only certain vessels carrying Certain Dangerous Cargoes, in bulk, will complete a Declaration of Security

for every evolution regardless of the MARSEC Level. At MARSEC Levels 2 and 3, all vessels and OCS facilities would need to complete the Declaration of Security.

OCS facilities that frequently receive the same vessel may execute a continuing Declaration of Security — a single Declaration of Security for multiple visits.

Each Declaration of Security must state the security activities for which the OCS facility and vessel are responsible during the vessel-to-facility interface. Declarations of Security must be kept as part of the OCS facility's recordkeeping.

Security Incident Procedures.

Each OCS facility must develop security incident procedures for responding to security incidents. The security incident procedures must explain the OCS facility's reaction to an emergency, including the notification and coordination with local, State, and federal authorities. The security incident procedures must also explain actions for securing the OCS facility as well as actions for evacuating passengers and crew.

Facility Security Assessment (FSA).

This interim rule requires all appropriate OCS facilities to complete a Facility Security Assessment, which is an essential part of the process of developing and

updating the required Facility Security Plan. The Facility Security Assessment is based in part on an on-scene security survey, which details the overall assessment of the OCS facility including any existing security measures, and includes a written report documenting the vulnerabilities and mitigation strategies of the OCS facility. As discussed in the interim rule "Implementation of National Maritime Security Initiatives" (USCG-2003-14792), 33 CFR 101.510, lists the various assessment tools that may be used to meet the risk assessment requirements in the parts 104 through 106 of this subchapter. The assessment tools listed are sufficient to enable the development of the Facility Security Plan. This list is also provided to ensure that the Facility Security Assessment is consistent with other modal assessments. We are working with other agencies to develop assessment tools that are sensitive to the diversity of the national Marine Transportation System to ensure consistent levels of security throughout the entire system. The designated Company Security Officer must conduct the on-scene survey by examining and evaluating existing OCS facility protective measures, procedures, and operations. Using the information obtained in the on-scene survey, the Company Security Officer must ensure the completion the Facility

Security Assessment. The Facility Security Assessment identifies and evaluates, in writing, existing security measures; key OCS facility operations; the likelihood of possible threats to key OCS facility operations; and weaknesses, including human factors in the infrastructure, policies, and procedures of the OCS facility.

The Facility Security Assessment includes, among other things, a written summary of how the assessment was conducted, each vulnerability found during the assessment, and countermeasures that could be used to address each vulnerability. The Facility Security Assessment must be reviewed and updated each time the Facility Security Plan is revised and when the Facility Security Plan is submitted for re-approval every five years

Facility Security Plan.

This interim rule requires each OCS facility owner or operator to develop an effective security plan that incorporates detailed preparedness, prevention, and response activities for each MARSEC Level, along with the organizations or personnel responsible for carrying out those activities. The requirements discussed in this part are consistent with the requirements covered in parts 104 and 105 of this subchapter.

The Facility Security Plan is a document, written in English that is prepared in response to the Facility Security Assessment and approved by the Coast Guard. A single Facility Security Plan may cover more than one OCS facility to the extent that they share physical characteristics and operations, if authorized and approved by the cognizant District Commander.

In addition to other things, the Facility Security Plan must respond specifically to any recommendations made by the Facility Security Assessment; must describe, for each MARSEC Level, how the OCS facility will apply the security measures required in these regulations; must detail the organizational structure of security for the OCS facility; must detail the responsibilities of all OCS facility personnel with a security duty; must detail the OCS facility's relationships with the Company, vessels that conduct operations with the OCS facility, and relevant authorities with a security responsibility; must provide for regular audit of the FSP and for its amendment in response to experience or changing circumstances; and must establish the procedures needed to assess the continuing effectiveness of security procedures and all security-related equipment and systems, including procedures for

identifying and responding to equipment or systems failure or malfunction.

Submission and Approval of Security Plan.

The Facility Security Plan, including the Facility Security Assessment report must, be submitted to and reviewed by the cognizant District Commander. Once the cognizant District Commander finds that the plan meets the security requirements in part 106, the submitter will receive confirmation via an approval letter.

If the cognizant District Commander requires more time than is indicated in the requirements of the interim rule to review a submitted Facility Security Plan, the cognizant District Commander may return to the submitter a written acknowledgement stating that the Coast Guard is currently reviewing the Facility Security Plan submitted for approval, and that the OCS facility may continue to operate so long as the OCS facility remains in compliance with the submitted Facility Security Plan.

If the cognizant District Commander finds that the FSP does not meet the security requirements, the plan would be returned to the OCS facility with either an approval letter stating conditions of the approval, or a disapproval letter along with an explanation of why the plan does not meet the part 106 requirements.

Security plans must be reviewed by the Coast Guard every time:

- The Facility Security Assessment is altered;
- Failures are identified during an exercise of the Facility Security Plan; and
- There is a change in ownership or operational control of the OCS facility or there are amendments to the Facility Security Plan.

Regulatory Assessment

This interim rule is a "significant regulatory action" under section 3(f) of Executive Order 12866, Regulatory Planning and Review, and has been reviewed by the Office of Management and Budget under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. It is significant under the regulatory policies and procedures of the Department of Homeland Security. A Regulatory Assessment is available in the docket as indicated under ADDRESSES. A summary of the Assessment follows:

Cost Assessment

For the purposes of good business practice or regulations promulgated by other Federal and State agencies, many companies already have spent a substantial amount of money and resources to upgrade and improve

security. The costs shown in this assessment do not include security measures these companies have already taken to enhance security.

The Coast Guard realizes that every company engaged in maritime commerce will not implement this interim rule exactly as presented in the assessment. Depending on each company's choices, some companies could spend much less than what is estimated herein while others could spend significantly more. In general, the Coast Guard assume that each company will implement this interim rule differently based on the types of OCS facilities it owns or operates and whether it engages in international or domestic trade.

This interim rule will affect about 40 OCS facilities under U.S. jurisdiction, (current and future facilities). These OCS facilities engage in exploring for, developing, or producing oil, natural gas, or mineral resources. To determine the number of OCS facilities, we used data that the Mineral Management Service (MMS) has identified as nationally critical OCS oil and gas infrastructure. These OCS facilities meet or exceed any of the following operational threshold characteristics:

(1) OCS facility hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;

(2) Production greater than 100,000 (one hundred thousand) barrels of oil per day; or

(3) Production greater than 200,000,000 (two hundred million) cubic feet of natural gas per day.

The estimated cost of complying with the interim rule is Present Value (PV) $37 million (2003–2012, 7 percent discount rate). In the first year of compliance, the cost of security assessments and plans, training, personnel, and paperwork is an estimated $3 million (non-discounted). Following initial implementation, the annual cost of compliance is an estimated $5 million (non-discounted).

Approximately 80 percent of the initial cost of the interim rule is for assigning and establishing Company Security Officers and Facility Security Officers, 12 percent is associated with paperwork creating Facility Security Assessments and Facility Security Plans, and 8 percent of the cost is associated with initial training (not including quarterly drills). Following the first year, approximately 58 percent of the cost is training (including quarterly drills), 42 percent is for Company Security Officers and Facility Security Officers, and less

than 1 percent is associated with paperwork. Annual training (including quarterly drills) is the primary cost driver of OCS facility security.

We estimated approximately 3,200 burden hours for paperwork during the first year of compliance (40 hours for each Facility Security Assessment and each Facility Security Plan). We estimated approximately 160 burden hours annually following full implementation of the interim rule to update Facility Security Assessments and Facility Security Plans.

We estimated the cost of this interim rule to be minimal in comparison to vessel and non-OCS facility security implementation. This interim rule includes only personnel, training, and paperwork costs for the affected OCS facility population. We assume the industry is adequately prepared with equipment suited to be used for security purposes (lights, radios, communications), therefore no security equipment installation, upgrades, or maintenance will be required for this interim rule.

Benefit Assessment

This interim rule is one of six interim rules that implement national maritime security initiatives concerning General Provisions, Area Maritime Security (ports), Vessels, Facilities, OCS Facilities, and AIS. The Coast

Guard used the National Risk Assessment Tool (N-RAT) to assess benefits that would result from increased security for vessels, facilities, OCS facilities, and ports. The N-RAT considers threat, vulnerability, and consequences for several maritime entities in various security-related scenarios. For a more detailed discussion on the N-RAT and how we employed this tool, refer to Applicability of National Maritime Security Initiatives in the interim rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register. For this benefit assessment, the Coast Guard used a team of experts to calculate a risk score for each entity and scenario before and after the implementation of required security measures. The difference in before and after scores indicates the benefit of the proposed action.

The Coast Guard recognized that the interim rules are a "family" of rules that will reinforce and support one another in their implementation. The Coast Guard has ensured, however, that risk reduction that is credited in one rulemaking is not also credited in another. For a more detailed discussion on the benefit assessment and how the Coast Guard addressed the potential to double-count the risk reduced, refer to Benefit Assessment in the interim

rule titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

The Coast Guard determined annual risk points reduced for each of the six interim rules using the N-RAT. The benefits are apportioned among the Vessel, Facility, OCS Facility, AMS, and AIS requirements. As shown in Table 1, the implementation of OCS Facility Security Plans for the affected population reduces 13,288 risk points annually through 2012. The benefits attributable for part 101, General Provisions, were not considered separately since it is an overarching section for all the parts.

Table 1. Annual Risk Points Reduced by the Interim Rules.

Maritime Entity	Annual Risk Points Reduced by Rulemaking				
	Vessel Security Plans	Facility Security Plans	OCS Facility Security Plans	AMS Plans	AIS
Vessels	778,633	3,385	3,385	3,385	1,448
Facilities	2,025	469,686	-	2,025	-
OCS Facilities	41	-	9,903	-	-
Port Areas	587	587	-	129,792	105
Total	781,285	473,659	13,288	135,202	1,553

Once we determined the annual risk points reduced, we discounted these estimates to their present value (seven percent discount rate, 2003-2012) so that they could be compared to the costs. We presented the cost effectiveness, or dollars per risk point reduced, in two ways: first, we compared the first-year cost and first-year benefit because first-year cost is the highest in our assessment as companies develop security plans and purchase equipment. Second, we compared the 10-year PV cost and the 10-year PV benefit. The results of our assessment are presented in Table 2.

Table 2. First-Year and 10-Year PV Cost and Benefit of the Interim Rules.

Item	Interim Rule				
	Vessel Security Plans	Facility Security Plans	OCS Facility Security Plans	AMS Plans	AIS*
First-Year Cost (millions)	$218	$1,125	$3	$120	$41
First-Year Benefit	781,285	473,659	13,288	135,202	1,553
First-Year Cost Effectiveness ($/Risk Point Reduced)	$279	$2,375	$205	$890	$26,391
10-Year PV Cost (millions)	$1,368	$5,399	$37	$477	$42
10-Year PV Benefit	5,871,540	3,559,655	99,863	1,016,074	11,671
10-Year PV Cost Effectiveness ($/Risk Point Reduced)	$233	$1,517	$368	$469	$3,624

*Cost less monetized safety benefit.

Small Entities

Under the Regulatory Flexibility Act (5 U.S.C. 601-612), the Coast Guard has considered whether this interim rule would have a significant economic impact on a substantial number of small entities. The term "small

entities" comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. This interim rule does not require a general notice of proposed rulemaking and, therefore, is exempt from the requirements of the Regulatory Flexibility Act. Although this interim rule is exempt, the Coast Guard has reviewed it for potential economic impacts on small entities. An Initial Regulatory Flexibility Analysis discussing the impact of this interim rule on small entities is available in the docket where indicated under ADDRESSES.

There are approximately 40 total current and future OCS facilities owned by 5 large companies that will be affected by this interim rule. Depending on how the corporate headquarters' operation is classified and whether it is oil or gas specific, these companies are generally classified under the North American Industry Classification System (NAICS) code 211111 or 221210. According to the Small Business Administration guidelines for these industries, a company with less than 500 total corporate employees is considered a small entity. The entities affected by this interim rule do not qualify as small entities because all of them have more than 500 employees.

Therefore, the Coast Guard certifies under 5 U.S.C. 605(b) that this interim rule will not have a significant economic impact on a substantial number of small entities. If you think that your business, organization, or governmental jurisdiction qualifies as a small entity and that this interim rule will have a significant economic impact on it, please submit a comment to the Docket Management Facility at the address under ADDRESSES. In your comment, explain why you think it qualifies and how and to what degree this interim rule would economically affect it.

Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104-121), we want to assist small entities in understanding this interim rule so that they can better evaluate its effects on them and participate in the rulemaking. If the interim rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please consult Lieutenant Greg Versaw, Coast Guard by telephone 202-267-1103, toll-free telephone 1-800-842-8740 ext. 7-1103, or electronic mail msregs@comdt.uscg.mil. Small businesses may send comments on the actions of Federal employees who

enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1-888-REG-FAIR (1-888-734-3247).

Collection of Information

This interim rule calls for a collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). As defined in 5 CFR 1320.3(c), "collection of information" comprises reporting, recordkeeping, monitoring, posting, labeling, and other, similar actions. The title and description of the information collections, a description of those who must collect the information, and an estimate of the total annual burden follow. The estimate covers the time for reviewing instructions, searching existing sources of data, gathering and maintaining the data needed, and completing and reviewing the collection. This interim rule modifies an existing OMB-approved collection--1625-0077 [formerly 2115-0551]. A summary of the revised collection follows.

TITLE: Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements.

OMB CONTROL NUMBER: 1625-0077

SUMMARY OF THE COLLECTION OF INFORMATION: The Coast Guard requires security standards for certain non-SOLAS Certificated MODUs and fixed and floating OCS platforms engaged in the exploration, production and development of oil and mineral resources on the OCS. This interim rule provides a framework to ensure adequate security planning, drilling, and communication procedures by requiring OCS facilities to develop and submit for approval Facility Security Assessments and Facility Security Plans. It also requires the use of a Declaration of Security between OCS facilities and certain vessels.

NEED FOR INFORMATION: The primary need for information is to identify the adequate security mitigating measures that will be implemented when needed.

PROPOSED USE OF INFORMATION: The information will be used to identify and communicate the security mitigating measures to the Coast Guard and necessary personnel. Declarations of Security will be used to identify and delineate the security responsibilities between an OCS facility and a vessel.

DESCRIPTION OF THE RESPONDENTS: OCS facilities that produce 100,000 (one hundred thousand) barrels of oil per day or 200,000,000 (two hundred million) cubic feet of natural gas per day or host more than 150 persons for 12 hours or more during a 24-hour period continuously for 30 days or more.

NUMBER OF RESPONDENTS: 40.

FREQUENCY OF RESPONSE: Varies.

Initial OCS Facility Security Assessments and OCS Facility Security Plans occur the first year the OCS facility is online with updates during each following year.

Depending on the OCS facility there may be additional requirements and reporting frequencies.

BURDEN OF RESPONSE: Development burden for the Facility Security Assessments and Facility Security Plans are estimated to be 80 hours for each OCS facility. Updating the assessments and plans is estimated to be 4 hours for some facilities and 2 hours for others. The Declaration of Security is expected to be 15 minutes each.

ESTIMATE OF TOTAL ANNUAL BURDEN: During the initial year the burden will be 3,200 hours. The average annual reporting burden to industry is 160 hours. For a summary of all revisions to this existing OMB-approved collection, refer to Collection of Information in the interim rule

titled "Implementation of National Maritime Security Initiatives" (USCG-2003-14792) published elsewhere in today's Federal Register.

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), we have submitted a copy of this interim rule to the Office of Management and Budget (OMB) for its review of the collection of information. Due to the circumstances surrounding this temporary rule, we asked for "emergency processing" of our request. We received OMB approval for the collection of information on June 16, 2003. It is valid until December 31, 2003.

We ask for public comment on the collection of information to help us determine how useful the information is; whether it can help us perform our functions better; whether it is readily available elsewhere; how accurate our estimate of the burden of collection is; how valid our methods for determining burden are; how we can improve the quality, usefulness, and clarity of the information; and how we can minimize the burden of collection.

If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under ADDRESSES, by the date under DATES.

You need not respond to a collection of information unless it displays a currently valid control number from OMB. We received OMB approval for the collection of information on June 16, 2003. It is valid until December 31, 2003.

Federalism

An interim rule has implications for federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. This part applies to facilities that are on the OCS, outside the jurisdiction of State waters or submerged lands. Nothing in this part will have a substantial direct effect on State or local governments, nor will a substantial direct cost of compliance be imposed on them. We have analyzed this interim rule under Executive Order 13132 and have determined that it therefore does not have implications for federalism.

Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the

expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of $100,000,000 or more in any one year. This interim rule is exempted from assessing the effects of the regulatory action as required by the Act because it is necessary for the national security of the United States (2 U.S.C. 1503(5)).

Taking of Private Property

This interim rule will not effect a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights.

Civil Justice Reform

This interim rule meets applicable standards in sections 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden.

Protection of Children

We have analyzed this interim rule under Executive Order 13045, Protection of Children from Environmental Health Risks and Safety Risks. While this interim rule is an economically significant rule, it does not create an environmental risk to health or risk to safety that may disproportionately affect children.

Indian Tribal Governments

This interim rule does not have tribal implications under Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, because it does not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

Energy Effects

We have analyzed this interim rule under Executive Order 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use. We have determined that it is not a "significant energy action" under that order. Although it is a "significant regulatory action" under Executive Order 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy. The Administrator of the Office of Information and Regulatory Affairs has not designated it as a significant energy action. Therefore, it does not require a Statement of Energy Effects under Executive Order 13211.

This interim rule has a positive effect on the supply, distribution, and use of energy. The interim rule provides

for security assessments, plans, procedures, and standards, which will prove beneficial for the supply, distribution, and use of energy at increased levels of maritime security.

Trade Impact Assessment

The Trade Agreement Act of 1979 (19 U.S.C. 2501-2582) prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety and security, are not considered unnecessary obstacles. The Act also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. We have assessed the potential effect of this interim rule and have determined that it would likely create obstacles to the foreign commerce of the United States. However, because these regulations are being put in place in order to further a legitimate domestic objective, to increase the security of the United States, any obstacles created by the regulation are not considered unnecessary obstacles.

Environment

We have considered the environmental impact of this interim rule and concluded that under figure 2-1, paragraph (34)(a) and (34)(c), of Commandant Instruction M16475.lD, this interim rule is categorically excluded from further

environmental documentation. This interim rule concerns security assessments, plans, training for personnel, and the establishment of security positions that will contribute to a higher level of marine safety and security for OCS facilities extracting oil or gas. A "Categorical Exclusion Determination" is available in the docket where indicated under ADDRESSES or SUPPLEMENTARY INFORMATION.

This rulemaking will not significantly impact the coastal zone. Further, the rulemaking and the execution of this interim rule will be done in conjunction with appropriate State coastal authorities. The Coast Guard will therefore, comply with the requirements of the Coastal Zone Management Act while furthering its intent to protect the coastal zone.

List of Subjects in 33 CFR Part 106

Facilities, Maritime security, Outer Continental Shelf, Security assessment, Security plan, Reporting and recordkeeping requirements.

For the reasons discussed in the preamble, the Coast Guard is adding part 106 to subchapter H of Title 33 of the CFR.

PART 106—OUTER CONTINENTAL SHELF (OCS) FACILITY SECURITY

Subpart A—General

Sec.

Subpart B—Outer Continental Shelf (OCS) Facility Security Requirements

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.

Subpart A—General

§ 106.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

§ 106.105 Applicability.

The requirements in this part apply to owners and operators of any fixed or floating facility, including MODUs not subject to part 104 of this subchapter, operating on the Outer Continental Shelf (OCS) of the United States for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources that are regulated by 33 CFR subchapter N, that meet the following operating conditions:

(a) Hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;

(b) Produces greater than 100,000 barrels of oil per day; or

(c) Produces greater than 200 million cubic feet of natural gas per day.

§ 106.110 Compliance dates.

(a) On or before [Insert date 180 days after publication in the Federal Register.], each Outer Continental Shelf (OCS) facility owner or operator must submit for each OCS facility a Facility Security Plan (FSP) described in subpart D of this part for review and approval to the cognizant District Commander.

(b) On or before [Insert date 360 days after publication in the Federal Register.], each OCS facility owner or operator must be operating in compliance with this part.

(c) OCS facilities built on or after July 1, 2004, must submit for approval an FSP 60 days prior to beginning operations.

§ 106.115 Compliance documentation.

Each OCS facility owner or operator subject to this part must ensure that no later than July 1, 2004, that copies of the following documentation are available at the OCS facility and are made available to the Coast Guard upon request:

(a) The approved Facility Security Plan (FSP) and any approved revisions or amendments thereto, and a letter of approval from the cognizant District Commander dated within the last 5 years;

(b) The FSP submitted for approval and current written acknowledgment from the cognizant District Commander, stating that the Coast Guard is currently reviewing the FSP submitted for approval and that the OCS facility may continue to operate so long as the OCS facility remains in compliance with the submitted FSP; or

(c) For OCS facilities operating under a Coast Guard-approved Alternative Security Program as provided in § 106.135, a copy of the Alternative Security Program the OCS facility is using and a letter signed by the OCS facility owner or operator, stating which Alternative Security Program the OCS facility is using and certifying that the OCS facility is in full compliance with that program.

§ 106.120 Noncompliance.

When an OCS facility is not in compliance with the requirements of this part, the OCS facility owner or operator must notify the cognizant District Commander and request a waiver to continue operations.

§ 106.125 Waivers.

Any OCS facility owner or operator may apply for a waiver of any requirement of this part that the OCS facility owner or operator considers unnecessary in light of the nature or operating conditions of the OCS facility.

A request for a waiver must be submitted in writing with justification to the cognizant District Commander. The cognizant District Commander may require the OCS facility owner or operator to provide additional data for use in determining the validity of the requested waiver. The cognizant District Commander may grant a waiver, in writing, with or without conditions only if the waiver will not reduce the overall security of the OCS facility, its personnel, or visiting vessels.

§ 106.130 Equivalents.

For any measure required by this part, the OCS facility owner or operator may propose an equivalent, as provided in § 101.130 of this subchapter.

§ 106.135 Alternative Security Program.

An OCS facility owner or operator may use an Alternative Security Program approved under § 101.120 of this subchapter if:

(a) The Alternative Security Program is appropriate to that OCS facility;

(b) The OCS facility does not serve vessels on international voyages; and

(c) The Alternative Security Program is implemented in its entirety.

§ 106.140 Maritime Security (MARSEC) Directive.

All OCS facility owners or operators subject to this part must comply with any instructions contained in a MARSEC Directive issued under § 101.405 of this subchapter.

§ 106.145 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in § 101.420 of this subchapter.

Subpart B—Outer Continental Shelf (OCS) Facility Security Requirements

§ 106.200 Owner or operator.

(a) Each OCS facility owner or operator must ensure that the OCS facility operates in compliance with the requirements of this part.

(b) For each OCS facility, the OCS facility owner or operator must:

(1) Define the security organizational structure for each OCS Facility and provide each person exercising security duties or responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate in writing, by name or title, a Company Security Officer (CSO) and a Facility Security Officer (FSO) for each OCS Facility and identify how those officers can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);

(5) Ensure that the OCS facility operates in compliance with the approved FSP;

(6) Ensure that adequate coordination of security issues takes place between OCS facilities and vessels, including the execution of a Declaration of Security (DoS) as required by this part;

(7) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required by the FSP for the new MARSEC Level; and

(8) Ensure all breaches of security and security incidents are reported in accordance with part 101 of this subchapter.

§ 106.205 Company Security Officer (CSO).

(a) General.--

(1) An OCS facility owner or operator may designate a single CSO for all its OCS facilities to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the OCS facilities for which each CSO is responsible.

(2) A CSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the CSO.

(3) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(b) Qualifications. The CSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Security administration and organization of the OCS facility;

(2) OCS facility and vessel operations and conditions;

(3) OCS facility and vessel security measures including the meaning and consequential requirements of the different MARSEC Levels;

(4) Emergency preparedness and response and contingency planning;

(5) Security equipment and systems and their operational limitations;

(6) Methods of conducting audits, inspection, control, and monitoring; and

(7) Techniques for security training and education, including security measures and procedures.

(c) In addition to the knowledge and training in paragraph (b) of this section, the CSO must have general knowledge, through training or equivalent job experience, in the following, as appropriate:

(1) Relevant international conventions, codes, and recommendations;

(2) Relevant government legislation and regulations;

(3) Responsibilities and functions of other security organizations;

(4) Methodology of Facility Assessment;

(5) Methods of OCS facility security surveys and inspections.

(6) Handling sensitive security information (SSI) and security related communications;

(7) Knowledge of current security threats and patterns;

(8) Recognition and detection of dangerous substances and devices;

(9) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(10) Techniques used to circumvent security measures;

(11) Methods of physical screening and non-intrusive inspections; and

(12) Conducting and assessing security drills and exercises.

(d) Responsibilities. In addition to any other duties required by this part, for each OCS facility for which the CSO is responsible, the CSO must:

(1) Keep the OCS facility apprised of potential threats or other information relevant to its security;

(2) Ensure that a Facility Security Assessment (FSA) is carried out in compliance with this part;

(3) Ensure that a Facility Security Plan (FSP) is developed, approved, maintained, and implemented in compliance with this part;

(4) Ensure that the FSP is modified when necessary to comply with this part;

(5) Ensure that OCS facility security activities are audited in compliance with this part;

(6) Ensure the timely correction of problems identified by audits or inspections;

(7) Enhance security awareness and vigilance within the owner's or operator's organization;

(8) Ensure relevant personnel receive adequate security training in compliance with this part;

(9) Ensure communication and cooperation between the OCS facility and vessels that interface with it, in compliance with this part;

(10) Ensure consistency between security requirements and safety requirements in compliance with this part;

(11) Ensure that if a common FSP is prepared for more than one similar OCS facility, the FSP reflects any OCS facility specific characteristics; and

(12) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate.

§ 106.210 OCS Facility Security Officer (FSO).

(a) General.--

(1) The FSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the FSO of each such OCS facility.

(2) The same person may serve as the FSO for more than one OCS facility, provided the facilities are within a reasonable proximity to each other. If a person serves as the FSO for more than one OCS facility, the name of each OCS facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each OCS facility for which is he or she is the FSO.

(3) The FSO may assign security duties to other OCS facility personnel; however, the FSO remains responsible for these duties.

(b) Qualifications. The FSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Those items listed in § 106.205 (b), and as appropriate § 106.205 (c), of this part;

(2) OCS facility layout;

(3) The FSP and related procedures; and

(4) Operation, testing and maintenance of security equipment and systems.

(c) Responsibilities. In addition to any other responsibilities specified elsewhere in this part, the FSO must, for each OCS facility for which he or she has been designated:

(1) Regularly inspect the OCS facility to ensure that security measures are maintained in compliance with this part;

(2) Ensure the maintenance of and supervision of the implementation of the FSP, and any amendments to the FSP, in compliance with this part;

(3) Ensure the coordination and handling of stores and industrial supplies in compliance with this part;

(4) Where applicable, propose modifications to the FSP to the Company Security Officer (CSO);

(5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

(6) Ensure security awareness and vigilance on board the OCS facility;

(7) Ensure adequate security training for OCS facility personnel in compliance with this part;

(8) Ensure the reporting and recording of all security incidents in compliance with this part;

(9) Ensure the coordinated implementation of the FSP with the CSO;

(10) Ensure that security equipment is properly operated, tested, calibrated and maintained in compliance with this part;

(11) Ensure consistency between security requirements and the proper treatment of OCS facility personnel affected by those requirements;

(12) Ensure that occurrences that threaten the security of the OCS facility are recorded and reported to the CSO;

(13) Ensure that when changes in the MARSEC Level are attained they are recorded and reported to the CSO, OCS

facility owner or operator, and the cognizant District Commander; and

(14) Have prompt access to a copy of the FSA, along with an approved copy of the FSP.

§ 106.215 Company or OCS facility personnel with security duties.

Company or OCS facility personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current security threats and patterns;

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Recognition of techniques used to circumvent security measures;

(e) Security related communications;

(f) Knowledge of emergency procedures and contingency plans;

(g) Operation of security equipment and systems;

(h) Testing, calibration, and maintenance of security equipment and systems;

(i) Inspection, control, and monitoring techniques;

(j) Methods of physical screenings of persons, personal effects, stores and industrial supplies;

(k) Relevant provisions of the Facility Security Plan (FSP); and

(l) The meaning and the consequential requirements of the different MARSEC Levels.

§ 106.220 Security training for all other OCS facility personnel.

All other OCS facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge, through training or equivalent job experience, of the following:

(a) Relevant provisions of the Facility Security Plan (FSP);

(b) The meaning and the consequential requirements of the different MARSEC Levels including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Recognition of techniques used to circumvent security measures.

§ 106.225 Drill and exercise requirements.

(a) General. Drills and exercises must test the proficiency of OCS facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(b) Drills.--

(1) From the date of the FSP approval, the FSO must ensure that at least one security drill is conducted every three months. Security drills may be held in conjunction with non-security drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the OCS facility, OCS facility personnel changes, the types of vessels calling at the OCS facility, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of appropriate authorities.

(3) If a vessel is conducting operations with the OCS facility on the date the OCS facility has planned to conduct any drills, the OCS facility may include, but cannot require, the vessel or vessel personnel to participate in the OCS facility's scheduled drill.

(c) Exercises.--

(1) From the date of the FSP approval, exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation;

(iii) Combined with other appropriate exercises held; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be facility-specific or part of a cooperative exercise program.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the Facility Security Plan and must include substantial and active participation of relevant company and OCS facility

personnel, and may include governmental authorities and vessels depending on the scope and the nature of the exercise.

§ 106.230 OCS facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized access, deletion, destruction, amendment, and disclosure. The following records must be kept:

(1) Training. For each security training session, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) Drills and exercises. For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, and any best practices or lessons learned which may improve the FSP;

(3) Incidents and breaches of security. Date and time of occurrence, location within the OCS facility, a description of the incident or breach, the identity of the

individual to whom it was reported, and a description of the response;

(4) Changes in MARSEC Levels. Date and time of the notification received, and the time of compliance with additional requirements;

(5) Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;

(6) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(7) Declaration of Security (DoS). A copy of each DoS for at least 90 days after the end of its effective period; and

(8) Annual audit of the Facility Security Plan (FSP). For each annual audit, a letter certified by the FSO stating the date the audit was conducted.

§ 106.235 Maritime Security (MARSEC) Level coordination and implementation.

(a) The OCS facility owner or operator must ensure the OCS facility operates in compliance with the security

requirements in this part for the MARSEC Level in effect for the OCS facility.

(b) When notified of an increase in the MARSEC Level, the OCS facility owner and operator must ensure:

(1) Vessels conducting operations with the OCS facility and vessels scheduled to arrive at the OCS facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security (DoS), if applicable, is revised as necessary;

(2) The OCS facility complies with the required additional security measures within 12 hours; and

(3) The OCS facility reports compliance or noncompliance to the cognizant District Commander.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer (FSO) must inform all OCS facility personnel about identified threats, emphasize reporting procedures, and stress the need for increased vigilance.

(d) An OCS facility owner or operator whose facility is not in compliance with the requirements of this section must so inform the cognizant District Commander and obtain approval prior to interfacing with another vessel or prior to continuing operations.

§ 106.240 Communications.

(a) The Facility Security Officer (FSO) must have a means to effectively notify OCS facility personnel of changes in security conditions at the OCS facility.

(b) Communication systems and procedures must allow effective and continuous communications between the OCS facility security personnel, vessels interfacing with the OCS facility, with the cognizant District Commander, and national and local authorities with security responsibilities.

(c) Facility communications systems must have a backup means for both internal and external communications.

§ 106.245 Procedures for interfacing with vessels.

The OCS facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

§ 106.250 Declaration of Security (DoS).

(a) Each OCS facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from vessels.

(b) At MARSEC Level 1, owners or operators of OCS facilities interfacing with a manned vessel carrying Certain Dangerous Cargoes, in bulk, must:

(1) Prior to the arrival of a vessel to the OCS facility, ensure the Facility Security Officer (FSO) and Master, Vessel Security Officer (VSO), or their designated representatives coordinate security needs and procedures, and agree upon the contents of a DoS for the period of time the vessel is at the OCS facility; and

(2) Upon the arrival of the vessel at the OCS facility, the FSO and Master, VSO, or their designated representatives, must sign the written DoS.

(c) Neither the OCS facility nor the vessel may embark or disembark personnel, or transfer stores or industrial supplies until the DoS has been signed.

(d) At MARSEC Levels 2 and 3, the FSOs of OCS facilities interfacing with manned vessels subject to part 104 must sign and implement DOSs.

(e) At MARSEC levels 1 and 2, FSOs of OCS facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for a specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.

§ 106.255 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in § 106.230(b)(5) of this part.

(c) The Facility Security Plan (FSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 106.260 Security measures for access control.

(a) General. The OCS facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction or dangerous substances and devices, including any device intended to damage or destroy persons, vessels, or the OCS facility;

(2) Secure dangerous substances and devices that are authorized by the OCS facility owner or operator to be on board; and

(3) Control access to the OCS facility.

(b) The OCS facility owner or operator must ensure that:

(1) All locations providing means of access to the OCS facility where access restrictions or prohibitions are applied for each security level to prevent unauthorized access;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them; and

(3) The means of identification required to allow individuals to access the OCS facility and remain on the OCS facility without challenge are established.

(c) The OCS facility owner or operator must ensure that an identification system is established for checking the identification of OCS facility personnel or other persons seeking access to the OCS facility that:

(1) Provides for identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems used by vessels conducting operations with the OCS facility;

(3) Is updated regularly; and

(4) Allows temporary or continuing access for OCS facility personnel and visitors through the use of a badge or other system to verify their identity.

(d) The OCS facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(e) MARSEC Level 1. The OCS facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Screen persons and personal effects going aboard the OCS facility for dangerous substances and devices at the rate specified in the approved FSP;

(2) Conspicuously post signs that describe security measures currently in effect and clearly stating that:

(i) Boarding an OCS facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to be on board;

(3) Check the identification of any person seeking to board the OCS facility, including OCS facility employees, passengers and crews of vessels interfacing with the OCS facility, vendors, and visitors;

(4) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of OCS facility personnel, to establish his or her identity or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(5) Deter unauthorized access to the OCS facility;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access;

(8) Ensure OCS facility personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other OCS facility personnel, unless security clearly requires it;

(9) Provide a designated secure area on board, or in liaison with a vessel interfacing with the OCS facility, for conducting inspections and screening of people and their personal effects; and

(10) Respond to the presence of unauthorized persons on board.

(f) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at

MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people and personal effects embarking onto the OCS facility as specified for MARSEC Level 2 in the approved FSP;

(2) Assigning additional personnel to patrol deck areas during periods of reduced OCS facility operations to deter unauthorized access;

(3) Limiting the number of access points to the OCS facility by closing and securing some access points; or

(4) Deterring waterside access to the OCS facility, which may include, providing boat patrols.

(g) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. The additional security measures may include:

(1) Screening all persons and personal effects for dangerous substances and devices;

(2) Being prepared to cooperate with responders;

(3) Limiting access to the OCS facility to a single, controlled access point;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending embarkation and/or disembarkation of personnel;

(6) Suspending the onloading of stores or industrial supplies;

(7) Evacuating the OCS facility; or

(8) Preparing for a full or partial search of the OCS facility.

§ 106.265 Security measures for restricted areas.

(a) General. The OCS facility owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be in the OCS facility;

(3) Protect the OCS facility;

(4) Protect vessels using and serving the OCS facility;

(5) Protect sensitive security areas within the OCS facility;

(6) Protect security and surveillance equipment and systems; and

(7) Protect stores and industrial supplies from tampering.

(b) Designation of restricted areas. The OCS facility owner or operator must ensure restricted areas are designated within the OCS facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The OCS facility owner or operator may designate the entire OCS facility as a restricted area. Restricted areas must include, as appropriate:

(1) Areas containing sensitive security information;

(2) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and

(3) Areas containing critical OCS facility infrastructure equipment, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Power distribution system;

(iv) Access points for ventilation and air-conditioning systems;

(v) Manufacturing areas and control rooms;

(vi) Areas designated for loading, unloading or storage of stores and industrial supplies; and

(vii) Areas containing hazardous materials.

(c) The OCS facility owner or operator must ensure that the Facility Security Plan (FSP) should include measures for restricted areas to:

(1) Identify which OCS facility personnel are authorized to have access;

(2) Determine which persons other than OCS facility personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area; and

(5) Define the times when access restrictions apply.

(d) MARSEC Level 1. At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Verifying the identification and authorization of all persons seeking entry;

(4) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry to or movement within restricted areas; or

(5) Designating temporary restricted areas to accommodate OCS facility operations. If temporary restricted areas are designated, the FSP must include security requirements to conduct a security sweep of the designated temporary restricted areas both before and after the area has been established.

(e) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Enhancing the effectiveness of the barriers surrounding restricted areas, for example, by the use of patrols or automatic intrusion detection devices;

(2) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(3) Further restricting access to the restricted areas and movements and storage within them;

(4) Using continuously monitored and recorded surveillance equipment;

(5) Increasing the number and frequency of patrols, including the use of waterborne patrols; or

(6) Restricting access to areas adjacent to the restricted areas.

(f) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas; or

(3) Searching restricted areas as part of a security sweep of all or part of the OCS facility.

§ 106.270 Security measures for delivery of stores and industrial supplies.

(a) General. The OCS facility owner or operator must ensure that security measures relating to the delivery of stores or industrial supplies to the OCS facility are implemented to:

(1) Check stores or industrial supplies for package integrity;

(2) Prevent stores or industrial supplies from being accepted without inspection;

(3) Deter tampering; and

(4) Prevent stores and industrial supplies from being accepted unless ordered. For any vessels that routinely use an OCS facility, an OCS facility owner or operator may establish and implement standing arrangements between the OCS facility, its suppliers, and any vessel delivering stores or industrial supplies regarding notification and the timing of deliveries and their documentation.

(b) MARSEC Level 1. At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of measures to:

(1) Inspect stores or industrial supplies before being accepted; and

(2) Check that stores or industrial supplies match the order prior to being brought on board.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved

Facility Security Plan (FSP). These additional security measures may include:

(1) Intensifying inspection of the stores or industrial supplies during delivery; or

(2) Checking stores or industrial supplies prior to receiving them on board.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Checking all OCS facility stores or industrial supplies more extensively;

(2) Restricting or suspending delivery of stores or industrial supplies; or

(3) Refusing to accept stores or industrial supplies on board.

§ 106.275 Security measures for monitoring.

(a) General.--

(1) The OCS facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards,

deck watches, waterborne patrols and automatic intrusion-detection devices, or surveillance equipment as specified in their approved Facility Security Plan (FSP), the:

(i) OCS facility;

(ii) Restricted areas on board the OCS facility; and

(iii) The area surrounding the OCS facility.

(2) The following must be considered when establishing the appropriate level and location of lighting:

(i) OCS facility personnel should be able to detect activities on and around OCS facility;

(ii) Coverage should facilitate personnel identification at access points; and

(iii) Lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(b) MARSEC Level 1. At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures, which may be implemented in coordination with a vessel interfacing with the OCS facility, to:

(1) Monitor the OCS facility, particularly OCS facility access points and restricted areas;

(2) Be able to conduct emergency searches of the OCS facility;

(3) Ensure that equipment or system failures or malfunctions are identified and corrected;

(4) Ensure that any automatic intrusion detection device, sets off an audible or visual alarm, or both, at a location that is continually attended or monitored; and

(5) Light deck and OCS facility access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the OCS facility.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of security patrols;

(2) Using (if not already in use) or increasing the use of security and surveillance equipment;

(3) Assigning additional personnel as security lookouts; or

(4) Coordinating with boat patrols, when provided.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Cooperating with responders;

(2) Switching on all lights;

(3) Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the OCS facility;

(4) Maximizing the length of time such surveillance equipment (if not already in use) can continue to record; or

(5) Preparing for underwater inspection of the OCS facility.

§ 106.280 Security incident procedures.

For each MARSEC Level, the OCS facility owner or operator must ensure the Facility Security Officer (FSO) and OCS facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical OCS facility and OCS facility-to-vessel interface operations;

(b) Deny access to the OCS facility, except to those responding to an emergency;

(c) Evacuate the OCS facility in case of security threats or breaches of security; and

(d) Report security incidents as required in § 101.305 of this subchapter;

(e) Brief all OSC facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(f) Secure non-critical operations in order to focus response on critical operations.

Subpart C—Outer Continental Shelf (OCS) Facility Security Assessment (FSA)

§ 106.300 General.--

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.

(b) A single FSA may be performed and applied to more than one OCS facility to the extent they share physical characteristics, location, and operations.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

(1) Knowledge of current and anticipated security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Recognition of techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on structures and essential services;

(7) OCS facility security requirements;

(8) OCS facility and vessel interface business practices;

(9) Contingency planning, emergency preparedness and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine or civil engineering; and

(13) OCS facility and vessel operations.

§ 106.305 Facility Security Assessment (FSA) requirements.

(a) Background. The OCS facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the OCS facility, including:

(i) The location of each access point to the OCS facility;

(ii) The number, reliability, and security duties of OCS facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The essential maintenance equipment and storage areas;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring OCS facility and vessel personnel;

(4) Procedures for controlling keys and other access prevention systems;

(5) Response capability for security incidents;

(6) Threat assessments, including the purpose and methodology of the assessment, for the OCS facility's location;

(7) Previous reports on security needs; and

(8) Any other existing security procedures and systems, equipment, communications, and OCS facility personnel.

(b) On-scene survey. The OCS facility owner or operator must ensure that an on-scene survey of each OCS facility is conducted. The on-scene survey examines and evaluates existing OCS facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) Analysis and recommendations. In conducting the FSA, the OCS owner or operator must ensure that the Company Security Officer (CSO) analyzes the OCS facility background information and the on-scene survey, and considering the

requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey, including but not limited to:

(i) Access to the OCS facility;

(ii) Structural integrity of the OCS facility;

(iii) Existing security measures and procedures, including identification systems;

(iv) Existing security measures and procedures relating to essential services;

(v) Measures to protect radio and telecommunication equipment, including computer systems and networks;

(vi) Existing agreements with private security companies;

(vii) Any conflicting policies between safety and security measures and procedures;

(viii) Any conflicting OCS facility operations and security duty assignments;

(ix) Any deficiencies identified during daily operations or training and drills; and

(x) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits.

(2) Possible security threats, including but not limited to:

(i) Damage to or destruction of the OCS facility or of a vessel adjacent to the OCS facility;

(ii) Smuggling dangerous substances and devices;

(iii) Use of a vessel interfacing with the OCS facility to carry those intending to cause a security incident and their equipment;

(iv) Use of a vessel interfacing with the OCS facility as a weapon or as a means to cause damage or destruction; and

(v) Nuclear, radiological, explosive, biological, and chemical attack;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the OCS facility's infrastructure, policies and procedures;

(5) Any particular aspects of the OCS facility, including the vessels that interface with the OCS facility, which make it likely to be the target of an attack;

(6) Likely consequences, in terms of loss of life, damage to property, or economic disruption, of an attack on or at the OCS facility; and

(7) Locations where access restrictions or prohibitions will be applied for each MARSEC Level.

(d) FSA Report.--

(1) The OCS facility owner or operator must ensure that a written FSA report is prepared and included as a part of the FSP. The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;

(iii) A description of each vulnerability found during the on-scene survey;

(iv) A description of security measures that could be used to address each vulnerability.

(v) A list of the key OCS facility operations that are important to protect; and

(vi) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the OCS facility.

(2) A FSA report must describe the following elements within the OCS facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems and networks; and

(vi) Essential services.

§ 106.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan (FSP) required in § 106.405 of this part.

(b) An OCS facility owner or operator may generate and submit a report that contains the FSA for more than one OCS facility subject to this part, to the extent that they share similarities in physical characteristics, location and operations.

Subpart D--Outer Continental Shelf (OCS) Facility Security Plan (FSP)

§ 106.400 General.

(a) The OCS facility owner or operator must ensure the FSO develops and implements a Facility Security Plan (FSP) for each OCS facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Facility Security Assessment (FSA);

(4) Must describe security measures for each MARSEC Level; and

(5) May cover more than one OCS facility to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the cognizant District Commander.

(b) The FSP must be submitted for approval to the cognizant District Commander in a written or electronic format in a manner prescribed by the cognizant District Commander.

(c) The FSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

§ 106.405 Format and content of the Facility Security Plan (FSP).

(a) An OCS facility owner or operator must ensure that the FSP consists of the individual sections listed in this paragraph. If the FSP does not follow the order as it appears in this paragraph, the OCS facility owner or

operator must ensure that the FSP contains an index identifying the location of each of the following sections:

(1) Security organization of the OCS facility;

(2) Personnel training;

(3) Drills and exercises;

(4) Records and documentation;

(5) Response to change in MARSEC Level;

(6) Procedures for interfacing with vessels;

(7) Declaration of Security (DoS);

(8) Communications;

(9) Security systems and equipment maintenance;

(10) Security measures for access control;

(11) Security measures for restricted areas;

(12) Security measures for delivery of stores and industrial supplies;

(13) Security measures for monitoring;

(14) Security incident procedures;

(15) Audits and FSP amendments; and

(16) Facility Security Assessment (FSA) report.

(b) The OCS facility owner or operator must ensure that the FSP describes in detail how each of the requirements of subpart B of this part will be met.

§ 106.410 Submission and approval.

(a) On or before [Insert date 180 days after publication in the Federal Register.], each OCS facility owner or operator must either:

(1) Submit one copy of the Facility Security Plan (FSP) for review and approval to the cognizant District Commander and a letter certifying that the FSP meets the applicable requirements of this part; or

(2) If implementing a Coast Guard approved Alternative Security Program, meet the requirements in § 101.120(b) of this subchapter.

(b) OCS facilities built on or after July 1, 2004, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations.

(c) The cognizant District Commander will examine each submission for compliance with this part, and return to the submitter either:

(1) A letter of approval, stating acceptance of the FSP and specifying any conditions of approval;

(2) An acknowledgement letter stating that the Coast Guard is currently reviewing the FSP submitted for approval, and that the OCS facility may continue to operate so long as the OCS facility remains in compliance with the submitted FSP; or

(3) A disapproval letter specifying the reasons for disapproval and the submitted FSP.

(d) An FSP may be submitted and approved to cover more than one OCS facility where they share similarities in physical characteristics, location, and operations.

(e) Each OCS facility owner or operator that submits one FSP to cover two or more OCS facilities of similar design, location, and operation must address OCS facility-specific information that includes the physical and operational characteristics of each OCS facility.

(f) An FSP that is approved by the cognizant District Commander is valid for 5 years from the date of its approval. The cognizant District Commander will issue an approval letter, as indicated in § 106.115 of this part.

§ 106.415 Amendment and audit.

(a) Amendments.--

(1) Amendments to a Facility Security Plan (FSP) that are approved by the cognizant District Commander may be initiated by:

(i) The OCS facility owner or operator; or

(ii) The cognizant District Commander, upon a determination that an amendment is needed to maintain the OCS facility's security. The cognizant District Commander will give the OCS facility owner or operator written notice

and request that the OCS facility owner or operator propose amendments addressing any matters specified in the notice. The OCS facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the OCS facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the cognizant District Commander.

(2) Proposed amendments must be sent to the cognizant District Commander. If initiated by the OCS facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant District Commander allows a shorter period. The cognizant District Commander will approve or disapprove the proposed amendment in accordance with § 106.410 of this subpart.

(3) If the owner or operator has changed, the Facility Security Officer (FSO) must amend the Facility Security Plan (FSP) to include the name and contact information of the new OCS facility owner(s) or operator(s) and submit the affected portion of the FSP for review and approval in accordance with § 106.410 of this subpart.

(b) Audits.--

(1) The FSO must ensure an audit of the FSP is performed annually, beginning no later than one year from the initial

date of approval and attach a letter to the FSP certifying that the FSP meets the applicable requirements of this part.

(2) If there is a change in ownership or operations of the OCS facility, or if there have been modifications to the OCS facility, the FSP must be audited including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the FSP as a result of modifications to the OCS facility may be limited to those sections of the FSP affected by the OCS facility modifications.

(4) Unless impracticable due to the size and nature of the company or the OCS facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

(i) Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require an amendment of either the Facility Security Assessment (FSA) or FSP, the FSO must submit, in accordance with § 106.410 of this subpart, the amendments to the cognizant District Commander for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

Date: June 23, 2003

THOMAS H. COLLINS
Admiral, U.S. Coast Guard
Commandant